RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: TPV-M03

Oops! EU Did It Again: How the Cyber Resilience Act Is Changing Open Source

Benjamin Bögel

Cabinet of the Executive Vice-President of the European Commission Henna Virkkunen
European Commission
https://www.linkedin.com/in/boegel/

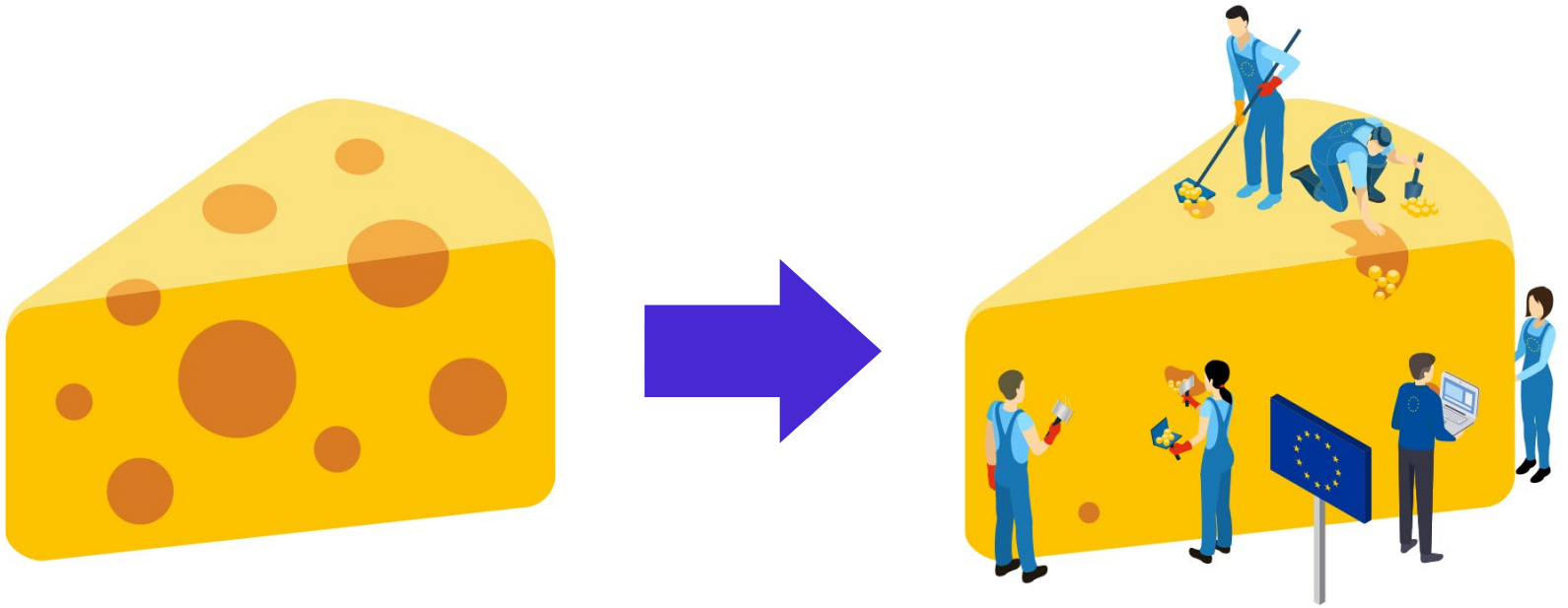
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

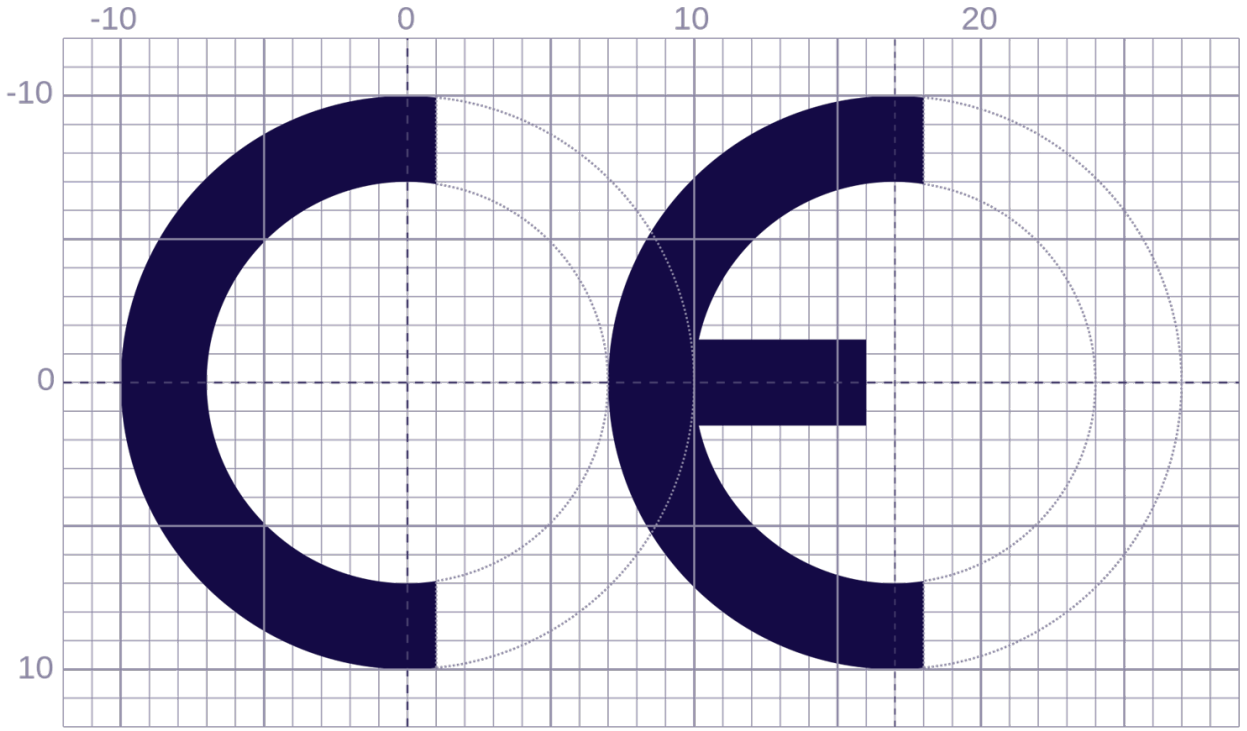
CRA In A Nutshell



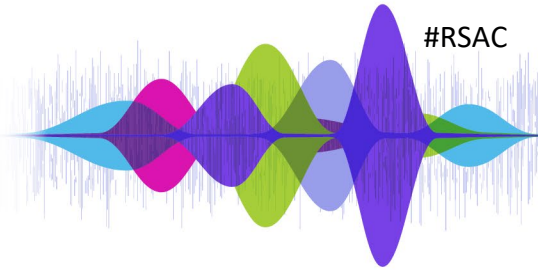
Main Elements Of The Legislation

- **Cybersecurity rules** for the “placing on the market” of hardware and software
- **Obligations** for manufacturers, distributors and importers
- Cybersecurity **essential requirements** across the life cycle
- Harmonised **standards** to follow
- **Conformity assessment** – differentiated by level of risk
- **Reporting** obligations
- **Market surveillance and enforcement**

CE Marking



Scope: “Products With Digital Elements”



✓ **Hardware products** (including components placed on the market)
(laptops, smart appliances, mobile phones, network equipment or CPUs…)

✓ **Software products** (including components placed on the market)
(operating systems, word processing, games or mobile apps, software libraries…)

…including their **remote data processing solutions**!

Outside The Scope

✗ **Non-commercial products**
(hobby products)

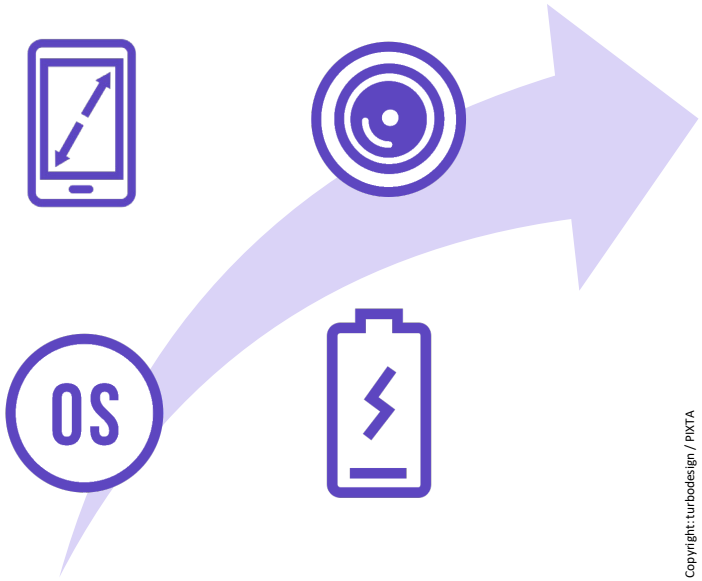
✗ **Services, in particular standalone SaaS** (covered by NIS2)
(websites, purely web-based offerings…)

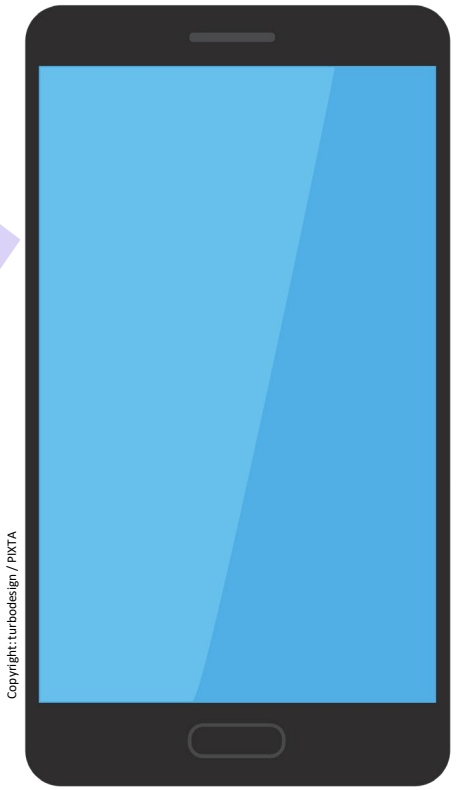
✗ **Outright exclusions**
(cars, medical devices, in vitro, certified aeronautical equipment, marine equipment)

A Simplified Example Of Smartphones

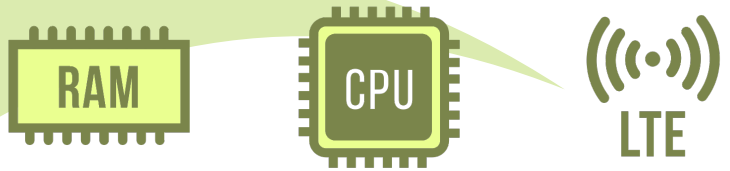
*As a rule, whoever places on the market a **"final" product or a component** is required to comply with the **essential requirements**, undergo **conformity assessment** and affix the **CE marking.***

Developed by the manufacturer placing the smartphone on the market:





Developed by upstream manufacturers for integration into the "final" product:

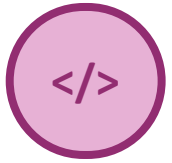


Conformity Assessment – Categories

Default category — self-assessment
(memory chips, mobile apps, smart speakers, computer games...)

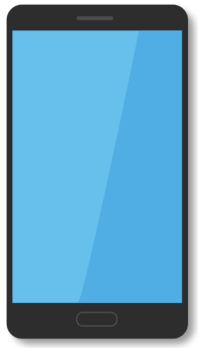
Important products — application of standards/third-party assessment
(operating systems, anti-virus, routers, firewalls…)

Critical products — in the future potentially certification
(smart cards, secure elements, smart meter gateways…)



Open source software — self-assessment (unless a “critical product”)
(web development frameworks, operating systems, database management systems…)

Sharing The Responsibility



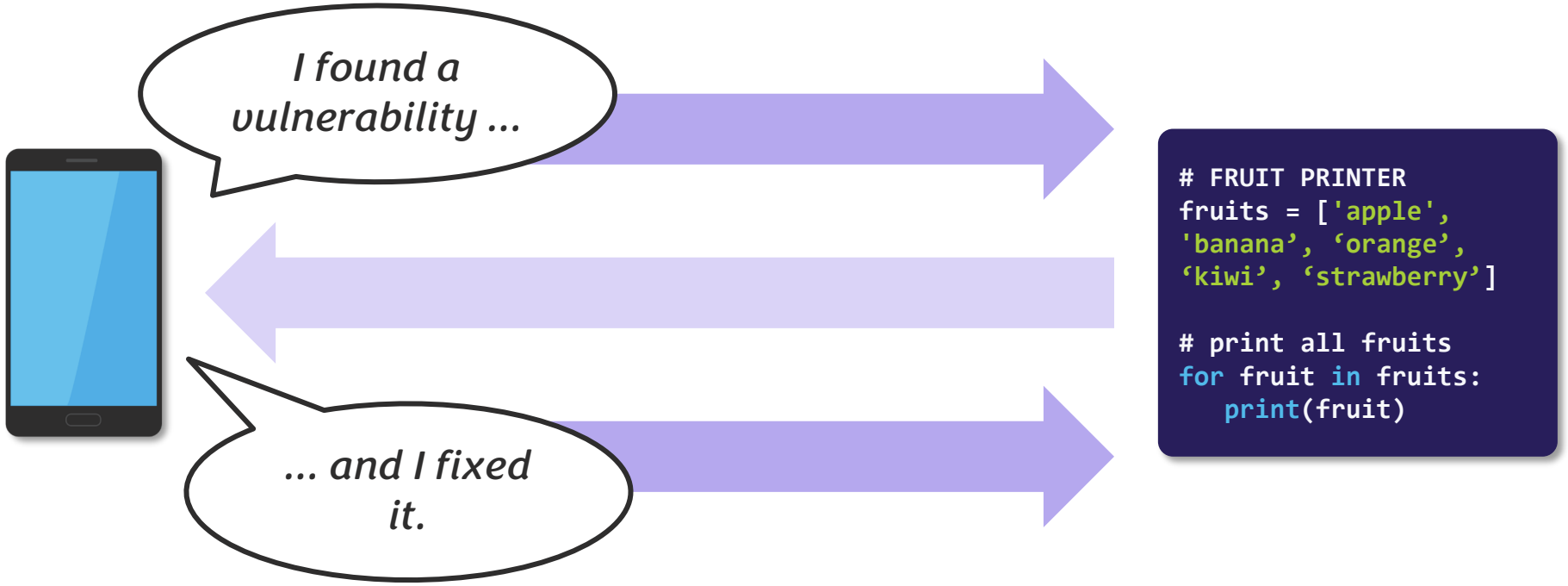

```
# FRUIT PRINTER
fruits = ['apple',
'banana', 'orange',
'kiwi', 'strawberry']

# print all fruits
for fruit in fruits:
   print(fruit)
```

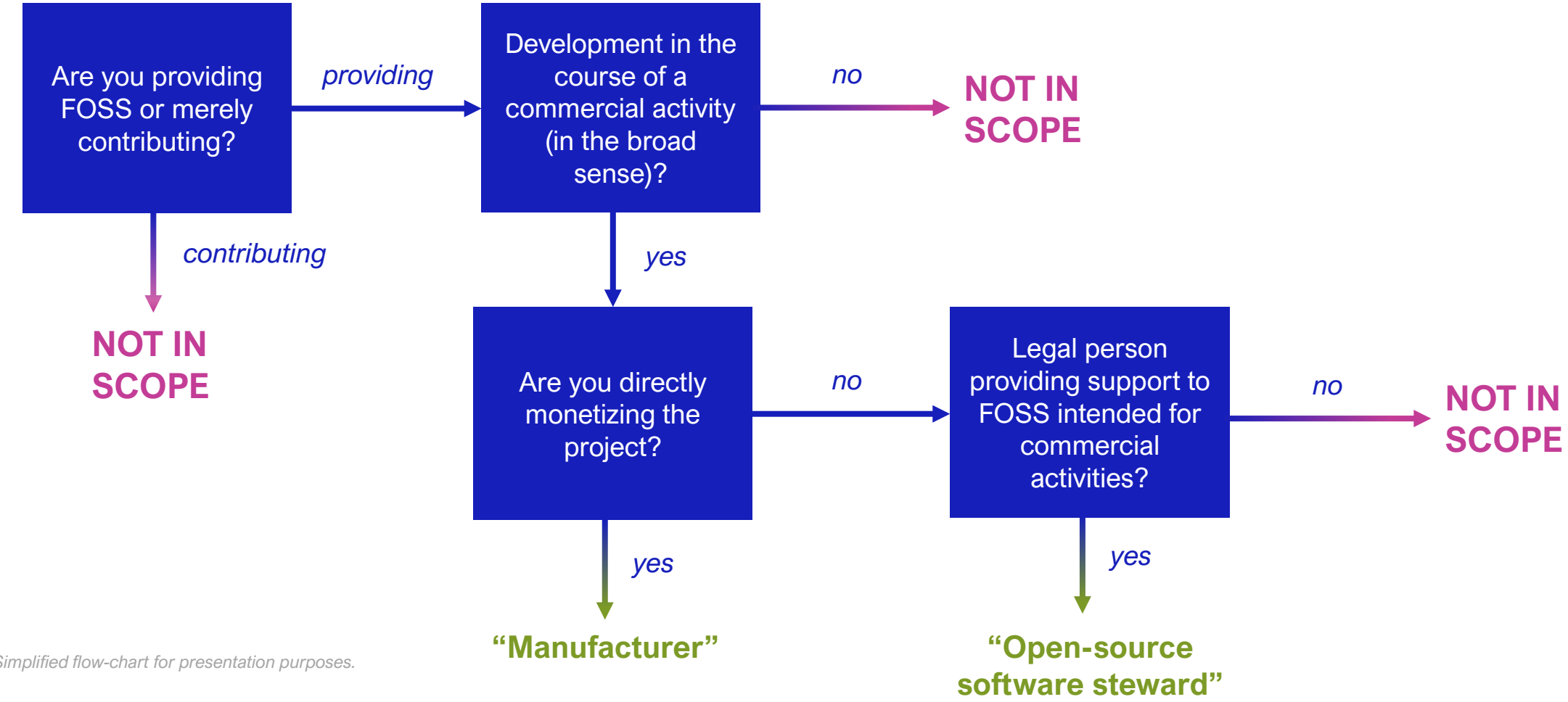
Sharing The Responsibility

I found a vulnerability ...
# FRUIT PRINTER
fruits = ['apple', 'banana', 'orange', 'kiwi', 'strawberry']
# print all fruits
for fruit in fruits:
print(fruit)

Sharing The Responsibility


I found a vulnerability ...
... and I fixed it.
# FRUIT PRINTER
fruits = ['apple', 'banana', 'orange', 'kiwi', 'strawberry']
# print all fruits
for fruit in fruits:
print(fruit)

Is Your Open Source Project Covered?*



* Simplified flow-chart for presentation purposes.

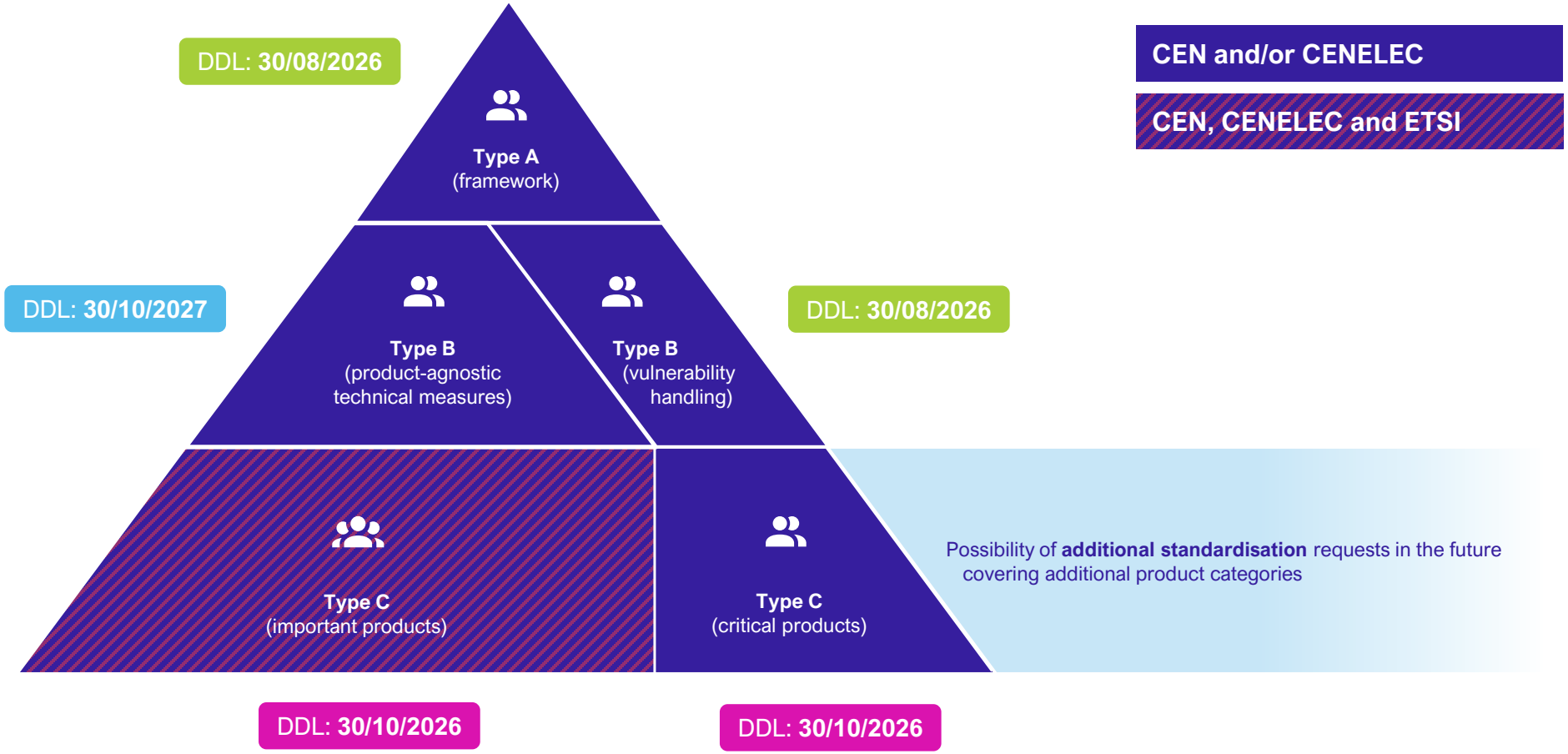
Open Source Software Steward

- **Light-touch approach** for legal persons that do not directly monetise but *"support on a sustained basis the development of specific [FOSS] products [..] intended for commercial activities".*
- **Examples:**
  - Foundations supporting specific FOSS projects
  - Companies that build FOSS for their use but make it public
  - Not-for-profit entities that develop FOSS

Obligations Of The Stewards

- Put in place a **cybersecurity policy** taking into account the specific nature of the open-source software steward
- Cooperate with the **market surveillance authorities** of the EU Member States
- **Report incidents and vulnerabilities** to the extent that they are involved in the development

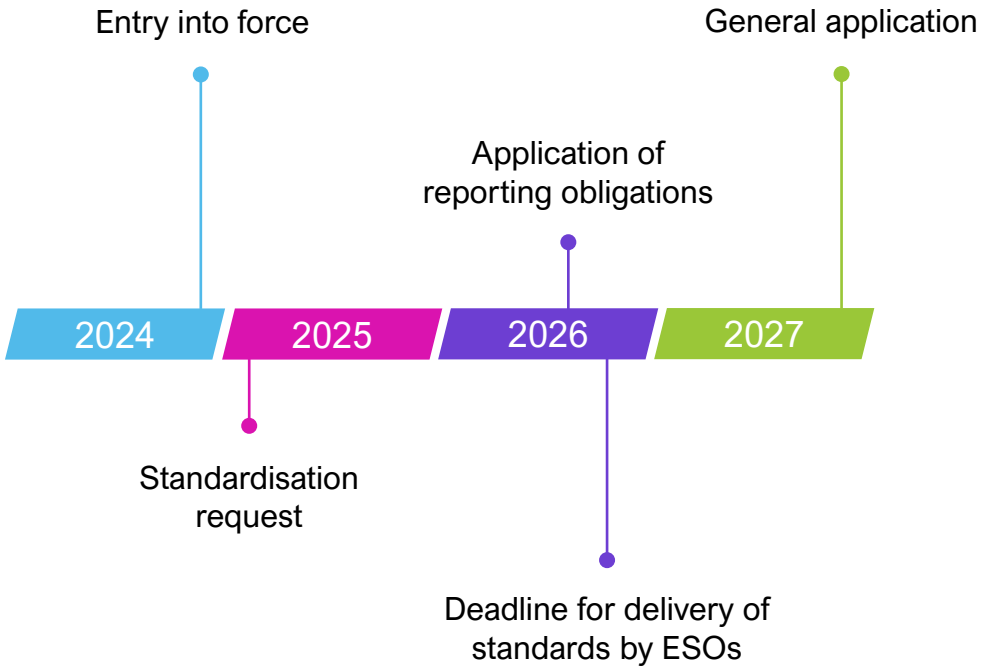
Standardisation Request In A Nutshell



Open Regulatory Compliance WG

AboutCode
Drupal
ERLANG ECOSYSTEM FOUNDATION
FreeBSD FOUNDATION
OpenInfra FOUNDATION
open robotics
OWASP
python
Ruby Central
Rust Foundation
Software Heritage
blender
NLNETLABS
Tauri
APACHE SOFTWARE FOUNDATION
LibreOffice The Document Foundation
matrix
The PHP Foundation

Timeline


Entry into force
General application
Application of reporting obligations
2024
2025
2026
2027
Standardisation request
Deadline for delivery of standards by ESOs

RSAC™ | 2025 Conference

Prepare For the CRA and Get Involved!

- Familiarize yourself with the Cyber Resilience Act and prepare for its implementation (https://europa.eu/!9N8TDV)
- Get involved in the standardisation process of CEN-CENELEC and ETSI
- Check out CYBERSTAND.eu
- Contribute to CRA-related open-source initiatives, such as the ORC WG

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you

For more information:

https://europa.eu/!9N8TDV